Method of highly effective protection from unauthorised use of software copies

Patent number:	DE4419115
Publication date:	1994-10-20
Inventor:	DOELKER MICHAEL (DE)
Applicant:	DOELKER MICHAEL (DE)
Classification:	
- international:	G06F12/14; G06K19/07
- european:	G06F1/00N5A2D2, G06F1/00N7R, G06F21/00N7P5H
Application number:	DE19944419115 19940601
Priority number(s):	DE19944419115 19940601

Abstract of **DE4419115**

The invention consists of a method of highly effective protection from unauthorised use of software copies, and is characterised by a co-ordinated combination of:

. an individually programmed memory or processor chip card, which functions as an authorisation chip card and
. a chip card reading device and
. software to be protected and
. a test program.

The effectiveness of the software protection is based on the immunity to falsification of memory and processor chip cards.
Since this method represents an economical and user-friendly solution, it is greatly superior to all methods which have been known until now for mass use.

---

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 19 115 A1**

(51) Int. Cl.[5]:
G 06 F 12/14
G 06 K 19/07

(21) Aktenzeichen: P 44 19 115.4
(22) Anmeldetag: 1. 6. 94
(43) Offenlegungstag: 20. 10. 94

DE 44 19 115 A1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

(71) Anmelder:
Dölker, Michael, 70619 Stuttgart, DE

(72) Erfinder:
gleich Anmelder

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum hochwirksamen Schutz vor unauthorisierter Benutzung von Softwarekopien

(57) Die Erfindung besteht in einem Verfahren zum hochwirksamen Schutz vor unautorisierter Benutzung von Softwarekopien und ist gekennzeichnet durch eine abgestimmte Kombination von
- individuell programmierter Speicher- oder Prozessor-Chipkarte, die als Autorisierungs-Chipkarte fungiert und
- einer Chipkarten-Lesevorrichtung, sowie
- einer zu schützenden Software und
- einem Prüfprogramm.

Die Wirksamkeit des Softwareschutzes basiert auf der Fälschungssicherheit von Speicher- und Prozessor-Chipkarten.
Da dieses Verfahren eine ökonomisch günstige und anwenderfreundliche Lösung darstellt, ist sie allen bisher bekannten Verfahren im Hinblick auf einen Masseneinsatz weit überlegen.

DE 44 19 115 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Beschreibung

Die Erfindung stellt ein Verfahren zum Schutz vor unerlaubter Benutzung von Software-Kopien dar.

Hauptsächlich die als sogenannte Standardsoftware im PC-Bereich bekannte Software verfügt über einen fehlenden oder unzureichenden Schutz gegen unberechtigtes Betreiben. Unter Berücksichtigung der enormen Schäden, die der Wirtschaft durch unberechtigtes Betreiben und Software-Piraterie entstehen, ist verständlich, daß verschiedenartige Anstrengungen unternommen worden sind, um Software zu schützen bzw. unberechtigtes Betreiben zu verhindern. In den einschlägigen Fachkreisen ist allgemein anerkannt, daß Software nicht hinreichend Software schützen kann. In die Software eingearbeitete Schutzroutinen oder -programme, die auf dem gleichen Speichermedium gespeichert sind wie das zu schützende Programm, können keinen vollständigen Schutz bieten, da sich derartige Disketten beispielsweise durch bitweises Kopieren unberechtigterweise vervielfältigen und dann betreiben lassen.

Deshalb wurde schon mehrfach versucht, durch zusätzliche spezielle Hardwarekomponenten den Schutz der Software zu erreichen. So zum Beispiel durch einen sogenannten "Dongle". Ein "Dongle" ist ein Stecker mit einem darin integrierten elektronischen Schaltkreis, der üblicherweise auf die Parallel-Schnittstelle des PC's gesteckt wird. Der elektronische Schaltkreis des Dongle beinhaltet einen Code, der elektronisch nicht kopierbar und veränderbar ist. Dieser Code wird durch eine spezielle Autorisierungsroutine des geschützten Anwenderprogramms gelesen, wenn dieses Anwenderprogramm aufgerufen wird. Falls dieser Code nicht gefunden wird, z. B., weil der "Dongle" nicht auf die parallele Schnittstelle des PC's aufgesteckt worden ist, ist das Anwenderprogramm nicht ablauffähig.

Bei vielen PC's ist dies kein gangbarer Weg zum Schutz der Software, da derartige "Dongles" zum Teil zu groß und zu teuer sind und darüber hinaus manche PC's häufig keine oder nicht-standardisierte parallele Schnittstellen aufweisen.

Eine weitere Möglichkeit des Schutzes besteht durch fest in der Hardware installierte Sicherheitsbausteine, die entsprechend gespeicherte Codes beinhalten, die vom Programm abgefragt werden. Es müssen in einem Rechner immer zwei Sicherheitsbausteine vorhanden sein, da in einem Handshakeverfahren gearbeitet wird. Am Anfang erzeugt ein Sicherheitsbaustein in sich eine Zufallszahl, die dann an den zweiten Sicherheitsbaustein übermittelt wird. Hier erfolgt eine weitere Verschlüsselung und die beiden Ergebnisse werden miteinander verglichen. Bei einer positiven Übereinstimmung wechseln beide Bausteine ihre Funktion und wiederholen die Prüfsequenz. Erst wenn diese zweite Überprüfung ebenfalls positiv ausfällt, öffnen sich die beiden Sicherheitsbausteine. Damit steht dem Computer die gesamte Software zur Verfügung.

Der Nachteil dieses Schutzes besteht darin, daß die gesamte Software, die geschützt werden soll, auf den Rechner abgestimmt werden muß, da die Programme die fest installierten Sicherheitsbausteine abfragen. Dies bedeutet, daß die Software auf keinem anderen Rechner ablauffähig ist.

Ein weiterer Versuch bestand darin, Steckkarten in das Rechnersystem zu installieren, die einen Datengenerator beinhalten, der mit der zu schützenden Software korrespondiert. Der entscheidende Nachteil besteht

hier ebenfalls darin, daß diese Steckkarten fest in den Rechner eingebaut werden und deshalb die Software nur auf diesem Rechnersystem ablauffähig ist. Dies geht zu Lasten der Flexibilität und Anwenderfreundlichkeit. Die Kosten für dieses Verfahren sind relativ hoch.

Aus den genannten Gründen hat sich de facto kein Verfahren für eine breite wirtschaftliche Anwendung gefunden. Die nachstehend beschriebene neue Verfahrensweise ist sowohl aus Sicht der einfachen technischen Realisierbarkeit als auch unter ökonomischen Aspekten ein gänzlich neuer Ansatz, da sie auf dem Einsatz von Speicher- oder Prozessor-Chipkarten beruht.

Der Erfindung liegt der Gedanke zugrunde, daß der Erwerber einer Software vom Hersteller eine Speicher- oder Prozessor-Chipkarte mitgeliefert bekommt.

Diese Chipkarte muß über einen in den Rechner integrierten oder extern angeschlossenen Chipkartenleser einem Prüfprogramm zugänglich gemacht werden, das von der zu schützenden Software aktiviert wird. Über das Prüfprogramm wird der Inhalt der Chipkarte gelesen. Wird der erwartete Inhalt vorgefunden, so gilt dies als korrekte Legitimierung für das Anwendungsprogramm. Wird keine Chipkarte vorgefunden oder ein anderer als der erwartete Inhalt, bricht das zu schützende Programm ab.

Die Speicher- oder Prozessor-Chipkarte kann vom Hersteller der Software nach seinen Anforderungen an die Schutzbedürftigkeit seines Produktes beliebig gestaltet werden.

So ist es möglich, daß jeder Softwarehersteller ein für sich günstiges Kosten/Nutzen-Verhältnis schafft.

Ein Verfahrensbeispiel für den Betrieb einer geschützten Software auf einem PC-System wird nachfolgend verbal und in der Zeichnung schematisch näher beschrieben.

Um die geschützte Software (4) auf dem Rechnersystem betreiben zu können, muß das Rechnersystem einmalig mit einer Chipkarten-Leseeinrichtung (2) ausgestattet werden. Da entsprechende Hardwarekomponenten am Markt zum Preis eines PC-Diskettenlaufwerkes erworben werden können und über eine Steckkarte einfach in ein bestehendes PC-System integrierbar sind, können die Hardwarevoraussetzungen schnell und kostengünstig geschaffen werden. Von der Gestaltung der Prüfroutinen in der zu schützenden Software ist es nun abhängig, ob bereits bei der Installation der Software auf der Festplatte oder aber erst beim Arbeiten mit der Software, auf das Vorhandensein der zur Software gehörenden Chipkarte (1) abgefragt wird. Findet die Prüfroutine keine oder nicht die richtige Chipkarte, so führt dies sofort oder nach n-Versuchen zum Abbruch. Das Verfahren funktioniert in gleicher Weise beim Betreiben der zu schützenden Software (4) von einem CD-ROM- (6) oder Diskettenlaufwerk (7).

Für ein reibungsloses Betreiben der geschützten Software ist es sinnvoll, wenn der Hersteller selbst Chipkartenleser zum Verkauf anbietet oder Chipkartenleser eines bestimmten Typs dem Anwender empfiehlt, da er so die Abstimmung der Prüfroutine in der Software auf die Treibersoftware des Chipkartenlesers vornehmen kann.

Ein wesentlicher Vorteil dieses Schutzverfahrens gegenüber früheren Entwicklungen für den Anwender besteht darin, daß

a) der Anwender Sicherungskopien jederzeit problemlos in unbegrenztem Umfang anfertigen kann (die Kopien sind jedoch ohne Chipkarte nicht ab-

lauffähig);
b) die Software auf mehreren Rechnersystemen installiert werden kann (aber nur auf dem Rechnersystem ablauffähig ist, das die Chipkarte vorfindet).

Dem Anwender wird hierdurch ein Höchstmaß an Flexibilität und Komfort geboten.

Ein wesentlicher Vorteil dieses Schutzverfahrens gegenüber früheren Entwicklungen für den Softwareentwickler besteht darin, daß

a) Speicher- und Prozessor-Chipkarten kostengünstig erworben werden können und somit zu keiner wesentlichen Verteuerung seines Produktes führen;
b) ein mißbräuchliches Duplizieren von Chipkarten in der Regel mit einem vertretbaren wirtschaftlichen Aufwand nicht möglich ist;
c) ein unberechtigtes Auslesen der Daten auf einer Chipkarte durch entsprechende interne Sicherheitseinrichtungen auf der Chipkarte verhindert werden kann;
d) je nach Schutzwürdigkeit der Software, der Sicherheitsgrad von ihm flexibel definiert werden kann und finanzieller Schaden durch Raubkopien weitestgehend abgewendet werden kann;
e) Chipkarten eine sehr hohe Ausfallsicherheit bieten, robust sind und damit für den häufigen Gebrauch geeignet sind;
f) der Softwarehersteller über das Prüfprogramm ein, auf die Chipkarte geschriebenes, Ablaufdatum für die Lizenz prüfen kann und so gegebenenfalls ein unberechtigtes Betreiben der Software, über ein im Lizenzvertrag festgeschriebenes Datum hinaus, verhindern kann.

Durch die in Fachkreisen allgemein bekannten Möglichkeiten, Speicher- und Prozessor-Chips gegen Mißbrauch zu schützen, ist die Wirksamkeit und der Sicherheitsgrad einzig und allein davon abhängig, welches Niveau der Softwareanbieter unter Berücksichtigung von Kosten/Nutzen erreichen möchte.

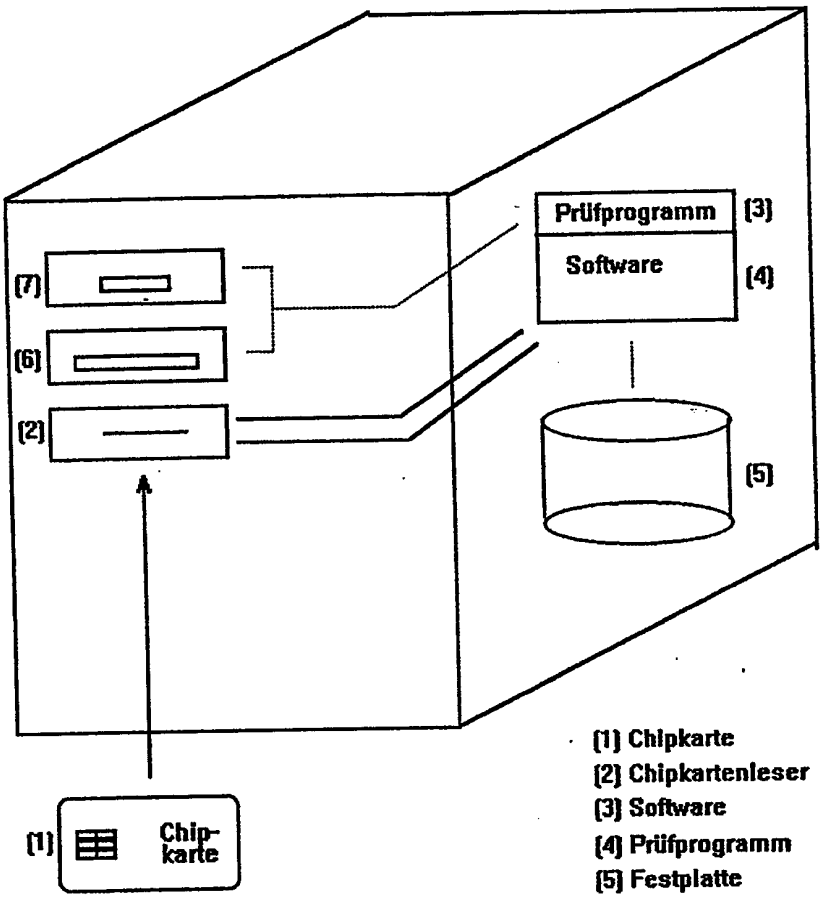
Zu Einzelheiten des Aufbaus und der Sicherheitsmerkmale von Chipkarten wird voll inhaltlich auf die Ausführungen in "Chipkarten als Sicherheitswerkzeuge" von Beutelspacher, Kersten, Pfau, erschienen im Springer Verlag 1991, Bezug genommen.

Patentansprüche

1. Verfahren zum hochwirksamen Schutz vor unauthorisierter Benutzung von Softwarekopien, **gekennzeichnet durch** eine abgestimmte Kombination von
   a) einer individuell programmierten Speicher- oder Prozessor-Chipkarte (1), die als Authorisierungs-Chipkarte fungiert und
   b) eine Chipkarten-Lesevorrichtung (2), die im Rechnersystem integriert oder über eine externe Schnittstelle am Rechner angeschlossen wird und
   c) einer auf einem Sekundärspeicher-Medium (5), (6) oder (7) zu schützenden Software (4) und
   d) einem von der zu schützenden Software aufgerufenen Prüfprogramm (3).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß dieses Schutzverfahren auf allen marktgängigen Rechnersystemen realisierbar ist.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Chipkartenlese-Vorrichtung für eine oder mehrere Chipkarten ausgelegt sein kann.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Speicher- oder Prozessor-Chipkarte ein Ablaufdatum für Software-Lizenzen enthalten kann.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 44 19 115 A1
Int. Cl.[5]: G 06 F 12/14
Offenlegungstag: 20. Oktober 1994



[1] Chipkarte
[2] Chipkartenleser
[3] Software
[4] Prüfprogramm
[5] Festplatte
[6] CD-ROM-Laufwerk
[7] Diskettenlaufwerk